

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-297510

(43)Date of publication of application : 11.10.2002

(51)Int.Cl.

G06F 13/00
G06F 12/00
G06F 12/14
G06F 17/30
H04L 12/58

(21)Application number : 2001-100186

(71)Applicant : RICOH CO LTD

(22)Date of filing : 30.03.2001

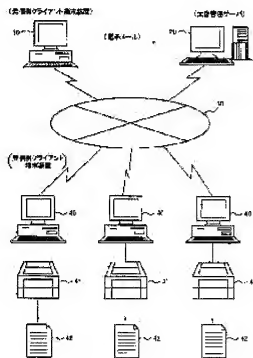
(72)Inventor : KON TSUTOMU

(54) DOCUMENT MANAGEMENT SYSTEM, PROGRAM AND RECORDING MEDIUM RECORDED WITH PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system that allows a user to read and print a document classified by a confidential level only if a password that enables the user to access a confidential document, the confidential level of which is higher than the classified documents, is inputted to the system.

SOLUTION: A system consists of a client transmission terminal 10, a document management server 20, and a client receiving terminal 40 with a printer, which are connected together via a network 30. The client transmission terminal 10 sets a confidential level to a document, sends a confidential document being attached to an electronic mail to the document management server 20 via the network 30, and stores the confidential document in the document management server 20. The system registers a password that enables a user to access the document classified by a confidential level that is higher than a corresponding level written on job descriptions in the document management server 20. The client receiving terminal 40 receives the stored confidential document from the document management server 20 only if the password is inputted, and then, the terminal can read or print the received confidential document.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-297510
(P2002-297510A)

(43) 公開日 平成14年10月11日 (2002.10.11)

(51) Int.Cl. ⁷	識別記号	F I	ページコード ⁸ (参考)
G 0 6 F 13/00	6 1 0	C 0 6 F 13/00	6 1 0 S 5 B 0 1 7
12/00	5 3 7	12/00	5 3 7 D 5 B 0 7 3
12/14	3 2 0	12/14	3 2 0 C 5 B 0 8 2
17/30	1 2 0	17/30	1 2 0 B 5 K 0 3 0
H 0 4 L 12/58	1 0 0	H 0 4 L 12/58	1 0 0 Z
審査請求 未請求 請求項の数14 O L (全 8 頁)			

(21) 出願番号 特願2001-100186(P2001-100186)

(22) 出願日 平成13年3月30日 (2001.3.30)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72) 発明者 今 勉

東京都大田区中馬込1丁目3番6号 株式
会社リコー内

(74) 代理人 100079843

弁理士 高野 明近 (外2名)

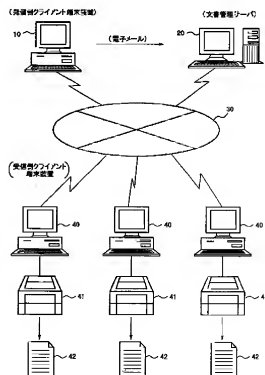
最終頁に続く

(54) 【発明の名称】 文書管理システム、プログラム及び該プログラムを記録した記録媒体

(57) 【要約】

【課題】 機密レベルが設定された文書を閲覧する際に、該機密レベル以上の文書にアクセス可能なパスワードが入力された時のみ機密文書の閲覧または印刷を行う。

【解決手段】 発信側クライアント端末装置10、文書管理サーバ20、受信側クライアント端末装置40とがネットワーク30を介して接続され、受信側クライアント端末装置40にはプリンタ41が接続されている。発信側クライアント端末装置10は、文書に機密レベルを設定し、その機密文書を電子メールに添付して文書管理サーバ20にネットワーク30を介して送信し、文書管理サーバ20にて該機密文書が記憶される。文書管理サーバ20に職務内容等に応じた機密レベル以上の文書にアクセス可能なパスワードを登録し、受信側クライアント端末装置40は、該パスワードが入力された時のみ文書管理サーバ20から記憶された機密文書を受信し、該受信した機密文書の閲覧または印刷を行うことができる。



【特許請求の範囲】

【請求項1】 電子メールを発信する発信側クライアント端末装置と、該電子メールを受信する受信側クライアント端末装置と、文書データを記憶可能な文書管理サーバとを有し、前記発信側クライアント端末装置と受信側クライアント端末装置と文書管理サーバとがネットワークを介して接続された文書管理システムにおいて、前記発信側クライアント端末装置にて作成された文書データに機密レベルを設定し、該機密レベルが設定された文書データを電子メールの添付ファイルとして前記文書管理サーバにネットワークを介して送信し、該送信された電子メールを該文書管理サーバにて記憶し、受信側クライアント端末装置は、前記機密レベル以上の文書データにアクセス可能なパスワードが入力された時のみ、前記文書管理サーバから前記記憶された電子メールがネットワークを介して転送され、該転送された電子メールに添付された前記機密レベル以下の文書データを閲覧、または印刷可能とすることを特徴とする文書管理システム。

【請求項2】 請求項1において、前記機密レベルが設定された文書データに対して更に閲覧のみ可能、または印刷まで可能とする処理レベルを設定し、前記受信側クライアント端末装置は、設定した処理レベルに応じて前記機密レベル以下の文書データを閲覧、または印刷可能であることを特徴とする文書管理システム。

【請求項3】 請求項1において、前記機密レベルは、前記受信側クライアントの職務内容に応じて設定されることを特徴とする文書管理システム。

【請求項4】 請求項1において、前記機密レベルは、前記受信側クライアントの部署に応じて設定されることを特徴とする文書管理システム。

【請求項5】 請求項1において、前記機密レベルは、前記受信側クライアントの株主の持ち株数に応じて設定されることを特徴とする文書管理システム。

【請求項6】 請求項1において、前記機密レベルに応じてパスワードを設定することを特徴とする文書管理システム。

【請求項7】 請求項1または6において、前記パスワードは、前記受信側クライアント端末装置で機密文書の閲覧、または印刷の都度入力されることを特徴とする文書管理システム。

【請求項8】 請求項1において、前記文書管理サーバは、前記受信側クライアント端末装置からの受信日時、または受信日時と印刷日時からなる受信情報をネットワークを介して受信し、受信した受信情報を発信側クライアント端末装置にネットワークを介して転送することを特徴とする文書管理システム。

【請求項9】 請求項1において、前記文書管理サーバは、前記受信側クライアント端末装置が機密文書を閲覧した後、または印刷した後は、該受信側クライアント端末装置から当該機密文書に対するアクセスを受け付けな

いことを特徴とする文書管理システム。

【請求項10】 請求項1において、前記受信側クライアント端末装置は、該受信側クライアント端末装置が機密文書を閲覧した後、または印刷した後に当該機密文書を削除可能とすることを特徴とする文書管理システム。

【請求項11】 請求項1ないし10のいずれかに記載された文書管理システムにおいて文書管理サーバを機能させるためのプログラム。

【請求項12】 請求項1ないし10のいずれかに記載された文書管理システムにおいて発信側クライアント端末装置を機能させるためのプログラム。

【請求項13】 請求項1ないし10のいずれかに記載された文書管理システムにおいて受信側クライアント端末装置を機能させるためのプログラム。

【請求項14】 請求項11ないし13のいずれかに記載されたプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、文書管理システム、プログラム及び該プログラムを記録した記録媒体、より詳細には、ネットワークを介して送受信される機密文書を保護することができる文書管理システム、該文書管理システムにおけるサーバ、クライアント端末として機能させるためのプログラム及び該プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】近年、例えば、インターネットや社内LANといったネットワークを利用した情報技術が著しく発達し、迅速な情報処理が行われるようになってきた。それに伴って企業等における、例えば、極秘、内幕、人事秘、社外秘といった企業内の機密文書もネットワークを介して行われるようになったが、その保護（セキュリティ）は万全ではなく外部に対して漏洩する可能性がある。

【0003】

【発明が解決しようとする課題】本発明は、上述の点に鑑みてなされたものであり、発信側クライアント端末装置にて作成した文書データに機密レベルを設定し、機密レベル以上の文書データにアクセス可能なパスワードを有する受信者のみが機密レベル以下の文書データの閲覧、または印刷可能とすること、

【0004】機密レベルが設定された文書データ（以下、機密文書データという）に対して閲覧のみ可能、または印刷まで可能とする処理レベルを設定し、その処理レベルに応じて機密文書データを閲覧、または印刷可能とすること、

【0005】機密文書データが閲覧、印刷された日時を受信側クライアント端末装置からネットワークを介して発信側クライアント端末装置に通知すること、

【0006】受信側クライアント端末装置により機密文書データの閲覧後、または印刷後に該機密文書データを削除可能とすること、を目的としてなされたものである。

【0007】

【課題を解決するための手段】請求項1の発明は、電子メールを発信する発信側クライアント端末装置と、該電子メールを受信する受信側クライアント端末装置と、文書データを記憶可能な文書管理サーバとを有し、前記発信側クライアント端末装置と受信側クライアント端末装置と文書管理サーバとがネットワークを介して接続された文書管理システムにおいて、前記発信側クライアント端末装置にて作成された文書データに機密レベルを設定し、該機密レベルが設定された文書データを電子メールの添付ファイルとして前記文書管理サーバにネットワークを介して送信し、該送信された電子メールを該文書管理サーバにて記憶し、受信側クライアント端末装置は、前記機密レベル以上の文書データにアクセス可能なパスワードが入力された時のみ、前記文書管理サーバから前記記憶された電子メールがネットワークを介して転送され、該転送された電子メールに添付された前記機密レベル以下の文書データを閲覧、または印刷可能とすること、を特徴としたものである。

【0008】請求項2の発明は、請求項1の発明において、前記機密レベルが設定された文書データに対して更に閲覧のみ可能、または印刷まで可能とする処理レベルを設定し、前記受信側クライアント端末装置は、設定した処理レベルに応じて前記機密レベル以下の文書データを閲覧、または印刷可能であることを特徴としたものである。

【0009】請求項3の発明は、請求項1の発明において、前記機密レベルは、前記受信側クライアントの職務内容に応じて設定されることを特徴としたものである。

【0010】請求項4の発明は、請求項1の発明において、前記機密レベルは、前記受信側クライアントの部署に応じて設定されることを特徴としたものである。

【0011】請求項5の発明は、請求項1の発明において、前記機密レベルは、前記受信側クライアントの株主の持ち株数に応じて設定されることを特徴としたものである。

【0012】請求項6の発明は、請求項1の発明において、前記機密レベルに応じてパスワードを設定することを特徴としたものである。

【0013】請求項7の発明は、請求項1または6の発明において、前記パスワードは、前記受信側クライアント端末装置で機密文書の閲覧、または印刷の都度入力されることを特徴としたものである。

【0014】請求項8の発明は、請求項1の発明において、前記文書管理サーバは、前記受信側クライアント端末装置からの受信日時、または受信日時と印刷日時から

なる受信情報をネットワークを介して受信し、受信した受信情報を発信側クライアント端末装置にネットワークを介して転送すること、を特徴としたものである。

【0015】請求項9の発明は、請求項1の発明において、前記文書管理サーバは、前記受信側クライアント端末装置が機密文書を閲覧した後、または印刷した後は、該受信側クライアント端末装置から当該機密文書に対するアクセスを受け付けないことを特徴としたものである。

【0016】請求項10の発明は、請求項1の発明において、前記受信側クライアント端末装置は、該受信側クライアント端末装置が機密文書を閲覧した後、または印刷した後に当該機密文書を削除可能とすることを特徴としたものである。

【0017】請求項11の発明は、請求項1ないし10のいずれかに記載された文書管理システムにおいて文書管理サーバを機能させるためのプログラムである。

【0018】請求項12の発明は、請求項1ないし10のいずれかに記載された文書管理システムにおいて発信側クライアント端末装置を機能させるためのプログラムである。

【0019】請求項13の発明は、請求項1ないし10のいずれかに記載された文書管理システムにおいて受信側クライアント端末装置を機能させるためのプログラムである。

【0020】請求項14の発明は、請求項1ないし13のいずれかに記載されたプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0021】

【発明の実施の形態】（実施例1）図1は、本発明が適用される文書管理システムの構成例を示す図で、図中、10は、発信側クライアント端末装置、20は、文書管理サーバ、30は、ネットワーク、40は、受信側クライアント端末装置、41は、プリンタ、42は、機密文書である。本実施例では、発信側クライアント端末装置10、文書管理サーバ20、複数台の受信側クライアント端末装置40とがネットワーク30を介して接続され、受信側クライアント端末装置40には、プリンタ41が接続されている。ネットワーク30は、例えば、社内LANやインターネットといったネットワークであり、本発明の文書管理システムは、インターネット等を介した社外との文書データの送受信にも適用することができる。

【0022】図2は、本発明における文書管理サーバ20と発信側クライアント端末装置10の内部構成例を示す図で、文書管理サーバ20は、文書データ記憶手段20a、機密文書データ認識手段20b、パスワード登録手段20c、レベル認識手段20d、電子メール転送手段20e、受信情報記憶手段20f、受信情報転送手段20g、通信制御手段20hとを有し、発信側クライ

ント端末装置10は、通信制御手段10a、機密文書データ設定手段10b、パスワード設定手段10c、レベル設定手段10d、電子メール送信手段10eとを有する。

【0023】文書データ記憶手段20aは、発信側クライアント端末装置10にて作成された文書データが添付された電子メールが電子メール送信手段10eによりネットワーク30を介して送信されると、送信されたこれらの文書データを記憶する。ここで、文書管理サーバ20にて発信側クライアント端末装置10から送信された文書データを、例えば、一般文書、機密文書といった分類をして記憶しておくこともできる。

【0024】機密文書データ認識手段20bは、発信側クライアント端末装置10の機密文書データ設定手段により機密文書データを認識する機能を有する。

【0025】パスワード登録手段20cは、機密文書データを受信可能な受信者のパスワードを予め登録しておく。ここで、機密文書データに対してアクセス可能な受信者にパスワードを割り当てる場合、例えば、部長、課長、係長といった社内の職務内容や、人事部、研究部、営業部のような部署（セクション）に応じて登録する。例えば、課長クラス以上でのみ閲覧を許可するパスワードのキャラクタとしてAxxxxxとすると、先頭のAによりその受信者が課長以上であることを認識することができる。また、パスワードの登録は、適宜変更することが可能である。また、受信者毎に任意のパスワードを職務内容や部署に関連付けておくことで、認識することもできる。こうしたことで、特定の役職の人間や特定のセクションの人間にのみ機密文書へのアクセスが許可されるため、セキュリティが保護される。また、受信側の電子メールアドレス等のID情報を発信側クライアントのアドレスリストとして登録しておくこともできる。

【0026】レベル認識手段20dは、発信側クライアント端末装置10のレベル設定手段10dにより設定された機密レベルと処理レベルとを認識する機能を有する。ここで、機密レベルとは、機密文書データに対してアクセス可能な受信者を制限するためのもので、前述したように、例えば、部長、課長、係長といった社内の職務内容や、人事部、研究部、営業部のような部署（セクション）に応じてレベル分けを行う。また、社外の場合にも、例えば、株主の持ち株数に応じてレベル分けを行うこともできる。また、処理レベルとは、機密文書データに対して実施する処理範囲を制限するためのもので、例えば、閲覧のみ可能で印刷は不可、または印刷まで可能といったように文書の機密密度に応じて実施できる処理を制限する。

【0027】電子メール転送手段20eは、発信側クライアント端末装置10からネットワーク30を介して送信された電子メールを受信側クライアント端末装置20へネットワーク30を介して転送する。

【0028】受信情報記憶手段20f及び受信情報転送手段20gは、受信側クライアント端末装置40からネットワーク30を介して送信された受信情報を記憶し、発信側クライアント端末装置10へ転送する機能を有する。ここで、受信情報とは、機密文書データの閲覧のみ許可された場合に、その文書データを受信した時の受信日時を示す情報、また、その文書データの印刷まで許可された場合、文書データの受信日時、印刷日時を示す情報のことである。これにより、発信側は、受信側が機密文書データを受信したかどうかを確認することができる。

【0029】通信制御手段20hは、ネットワーク30に接続してサーバや他のクライアント端末装置とデータの送受信を行う。

【0030】図3は、本発明における受信側クライアント端末装置40の内部構成例を示す図で、受信側クライアント端末装置40は、通信制御手段40a、パスワード入力手段40b、受信情報転送手段40c、機密文書データ削除手段40dとを有する。ここで、前述した発信側クライアント端末装置10と受信側クライアント端末装置40は、同様の機能を有しており、ネットワーク30に接続されているクライアント端末装置であれば、電子メール等の送受信を相互に行うことができる。

【0031】パスワード入力手段40bは、受信者のパスワードを入力する機能を有し、機密レベル以上の文書データにアクセス可能なパスワードが入力されると、文書管理サーバ20において、登録されたパスワードと照合され、パスワードが合致した場合、記憶された機密文書データを文書管理サーバ20から受信側クライアント端末装置40に転送し、設定された処理レベルに応じて閲覧、印刷することが可能となる。

【0032】受信情報転送手段40cは、上記処理レベルにより機密文書データの閲覧のみ許可された場合に、その機密文書データを受信した時の受信日時を文書管理サーバ20にネットワーク30を介して送信し、機密文書データの閲覧、印刷まで許可された場合、機密文書データの受信日時、印刷日時を文書管理サーバ20にネットワーク30を介して送信する。文書管理サーバ20は、これらの受信情報を発信側クライアント端末装置10に転送する。

【0033】機密文書データ削除手段40dは、機密文書データを閲覧した後、または印刷した後に機密文書データを削除する機能を有し、企業内ネットワークに適用する場合、企業内の取り決めに基づいて、例えば、機密文書データに予めフラグ信号等を付加しておいて、機密文書データが閲覧、または印刷された時に削除できるように設定しておいてもよい。また、他の削除手段として、文書管理サーバ20から受信側クライアント端末装置40内の機密文書データを削除することもできる。この場合、文書管理サーバ20が受信側クライアント端末装置40を特定するために、機密文書データの閲覧後、

または印刷後に、クライアント端末装置固有のIPアドレスや機器番号等を文書管理サーバ20へ送信して、クライアント端末装置を特定して、該当する機密文書データを削除するようにする。また、受信側にて閲覧、または印刷後に適宜、削除するようにしてもよい。このように、機密文書データを削除することで、機密文書のむやみな漏洩を防止することができる。

【0034】また、受信側が機密文書データを閲覧した後、または印刷した後に受信側クライアント端末装置40から当該機密文書データに対するアクセスを文書管理サーバ20が受け付けないようにすることもできる。

【0035】図4は、本発明における機密文書データが添付された電子メールの送信画面の一例を示す図で、図中、50は、電子メールの送信画面、該電子メールの送信画面50は、送信ボタン51、機密文書設定欄52、パスワード設定欄53、機密レベル及び処理レベル設定欄54、宛先欄55、添付ファイル欄56、発信元欄57を有する。本例では、発信側により機密文書設定欄52で機密文書に設定され、パスワード設定欄53でパスワード有りに設定されている。機密レベル設定は、機密度に応じて一般、レベル1、レベル2、・・・と高くなる。一般に設定された場合、誰でも閲覧、プリントアウトが可能であり、パスワード設定がある場合は、パスワードさえ入力すればあとの制限はない。レベル1以降は、それぞれのレベルに対して閲覧のみ可能、またはプリントアウトまで可能の中から発信者が選択して処理レベルを設定する。ここでは、閲覧のみが設定されている。

【0036】さらに、宛先欄55に宛先、CC、件名を入力し、作成した機密文書データを添付ファイル欄56に添付する。そして、送信ボタン51をクリックすると、電子メールがネットワーク30を介して文書管理サーバ20に送信され、文書管理サーバ20にて送信された電子メールが記憶される。

【0037】受信側クライアント端末装置40からネットワーク30を介して文書管理サーバ20に接続し、受信側が、文書管理サーバ20に記憶された電子メールにアクセスし、受信側により添付ファイル欄56に添付されたファイルがクリックされると、パスワード入力欄58が表示され、例えば、機密レベルのレベル1として課長クラス以上にのみアクセス可能に設定されている場合、課長クラス以上に設定されたパスワードを有する受信者がパスワードを入力して、設定された処理レベルに応じて機密文書データを閲覧、または印刷することができる。この時、受信した日時、例えば、3/29、15:45といった受信情報が受信側クライアント端末装置40から文書管理サーバ20にネットワーク30を介して送信され、文書管理サーバ20にて記憶される。記憶された受信情報は、文書管理サーバ20からネットワーク30を介して発信側クライアント端末装置10に

転送される。

【0038】(実施例2)図5は、本発明が適用される文書管理システムの他の構成例を示す図で、図中、21は、プリンタサーバで、該プリンタサーバ21は、ネットワーク30を介して発信側クライアント端末装置10、文書管理サーバ20、受信側クライアント端末装置40とが接続されている。本実施例では、プリンタサーバ21により複数のプリンタ41が管理されている。ただし、本発明は、図1、図5に示した文書管理システムの構成例に限定されず、他のシステム構成にも適用することができる。

【0039】以上、本発明の文書管理システムにおける各実施形態を説明してきたが、本発明は、上記文書管理システムの各機能を実現させるために、文書管理サーバ20、発信側クライアント端末装置10、受信側クライアント端末装置40としてそれぞれ機能させるためのプログラムとしての形態も可能である。ここで、発信側クライアント端末装置10と受信側クライアント端末装置40とが同じプログラムを有するようにして相互に送受信する形態も可能である。

【0040】本発明による文書管理の機能を実現するためのプログラムやデータを記録した記録媒体の実施形態を説明する。記録媒体としては、具体的には、CD-ROM、光磁気ディスク、DVD-ROM、フロッピー（登録商標）ディスク、フラッシュメモリ、メモリーカード、やメモリスティック及びその他各種ROMやRAM等が想定でき、これら記録媒体に上述した本発明の各実施形態のシステムの機能をコンピュータに実行させ、文書管理の機能を実現するためのプログラムを記録して流通させることにより、当該機能の実現を容易にする。そしてコンピュータ等の情報処理装置に上記のごとくの記録媒体を装着して情報処理装置によりプログラムを読み出すか、若しくは情報処理装置が備えている記憶媒体に当該プログラムを記憶させておき、必要に応じて読み出すことにより、本発明に関わる文書管理機能を実行することができる。

【0041】

【発明の効果】本発明によると、発信側クライアント端末装置にて作成した文書データに機密レベルを設定し、機密レベル以上の文書データにアクセス可能なパスワードを有する受信者のみが機密レベル以下の文書データの閲覧、または印刷可能とすることにより、機密文書のセキュリティが強化でき、むやみな漏洩を防ぐことができる。

【0042】機密レベルが設定された文書データに対して閲覧のみ可能、または印刷まで可能とする処理レベルを設定し、その処理レベルに応じて機密レベルが設定された文書データを閲覧、または印刷可能とすることにより、機密文書のセキュリティを強化することが可能となる。

【0043】機密文書データが閲覧、印刷された日時を受信側クライアント端末装置からネットワークを介して発信側クライアント端末装置に通知することで、発信側で受信側にて機密文書を受信したことが確認できる。

【0044】受信側クライアント端末装置により機密文書データの閲覧後、または印刷後に該機密文書データを削除可能とすることで、むやみな漏洩を防ぐことができる。

【図面の簡単な説明】

【図1】 本発明が適用される文書管理システムの構成例を示す図である。

【図2】 本発明における文書管理サーバと発信側クライアント端末装置の内部構成例を示す図である。

【図3】 本発明における受信側クライアント端末装置の内部構成例を示す図である。

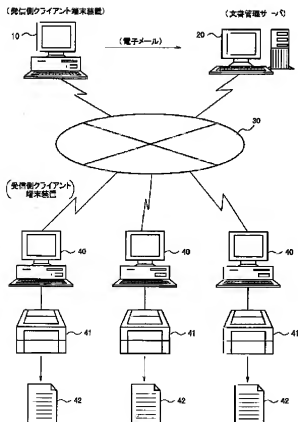
【図4】 本発明における機密文書データが添付された電子メールの送信画面の一例を示す図である。

【図5】 本発明が適用される文書管理システムの他の構成例を示す図である。

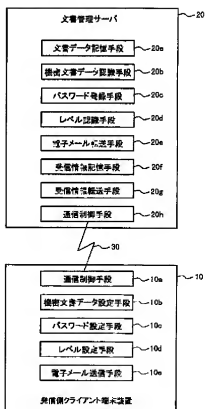
【符号の説明】

10…発信側クライアント端末装置、10a…通信制御手段、10b…機密文書データ設定手段、10c…パスワード設定手段、10d…レベル設定手段、10e…電子メール送信手段、20…文書管理サーバ、20a…文書データ記憶手段、20b…機密文書データ認識手段、20c…パスワード登録手段、20d…レベル認識手段、20e…電子メール転送手段、20f…受信情報記憶手段、20g…受信情報転送手段、20h…通信制御手段、21…プリンタサーバ、30…ネットワーク、40…受信側クライアント端末装置、40a…通信制御手段、40b…パスワード入力手段、40c…受信情報送信手段、40d…機密文書データ削除手段、41…プリンタ、42…機密文書、50…電子メールの送信画面、51…送信ボタン、52…機密文書設定欄、53…パスワード設定欄、54…機密レベル及び処理レベル設定欄、55…宛先欄、56…添付ファイル欄、57…発信元欄、58…パスワード入力欄。

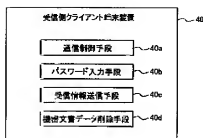
【図1】



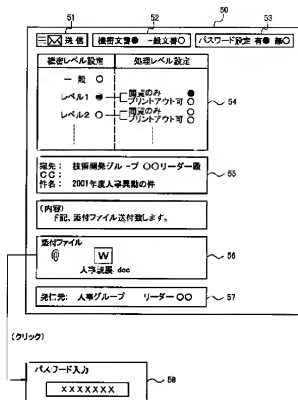
【図2】



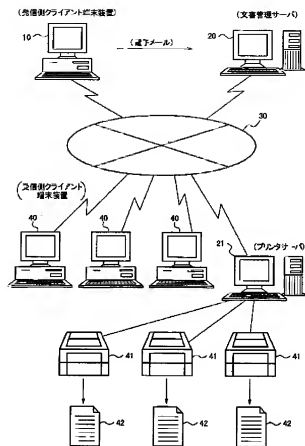
【図3】



【図4】



【図5】



フロントページの続き

Fターム(参考) 5B017 AA03 BA05 CA16
 5B075 KK43 KK54 KK63 UU06
 5B082 AA00 EA12
 5K030 GA15 HA08 HC01 JT03 KA01
 KA06 KA13 LD11 LD19 MB18